T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

SAMPLE

Occupational specialism assessment (OSA)

Cyber Security

Assignment 2

Assignment brief

v1.1: Specimen assessment materials
21 November 2023
603/6901/2

Internal reference: DSS-0013-03

NCFE

T Level Technical Qualification in Digital Support Services Occupational specialism assessment (OSA)

Cyber Security

Assignment brief

Assignment 2

SAMPLE

Contents

About this assignment

Introduction

This assignment is set by NCFE and administered by your provider over one week. The times and dates will be specified by NCFE.

The assignment will be completed under supervised conditions.

You must complete all tasks in this assignment independently. You are required to sign a declaration of authenticity to confirm that the work is your own. This is to ensure authenticity and to prevent potential malpractice and maladministration. If any evidence was found not to be your own work, it could impact your overall grade.

Internet access is allowed for tasks 1 and 2.

Ensure all print screens have been labelled with a brief description of what is being shown.

Save your work regularly as you work through the assessment.

Submit the work as a single .pdf file at the end of the assessment.

Electronic files should be named using the following format for identification purposes – Surname_Initial_student number_evidence reference.

For example: ‘Smith_J_123456789_Task1’.

Timing

You have 10 hours to complete all tasks within this assignment. Each task has the following number of hours:

Task 1 – 7 hours 30 minutes (this will be completed in 2 sessions)

Task 2 – 2 hours 30 minutes (this will be completed in 1 session)

Individual tasks must be completed within the timescales stated for each task, but it is up to you how long you spend on each part of the task, therefore be careful to manage your time appropriately.

Marks available

Task 1 – 42 marks

Task 2 – 18 marks

Details on the marks available are provided in each task.

You should attempt to complete all the tasks.

Read the instructions provided carefully.

SAMPLE

Performance outcomes (POs)

Marks will be awarded against the skills and knowledge performance outcomes (POs) as follows:

Task 1

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (24 marks)

PO2: Propose remediation advice for a security risk assessment (18 marks)

(42 marks)

Task 2

PO3: Discover, evaluate and apply reliable sources of knowledge (18 marks)

(18 marks)

SAMPLE

Scenario

Brief

Tony is a remote worker who has worked in the customer services support team for 6 months.

He has found that the software programs he is working with are running extremely slowly. Although he does not believe he has used any websites that are not secure, he has received and opened three emails and their attachments. He is now concerned that there is an issue with his laptop that he cannot resolve.

Tony usually works remotely, logging into public or private internet when necessary. Today however he is working from head office and so has been logged into the main system.

The IT manager has not noticed any issues with the main system but is aware of the problem with Tony's laptop and needs to ensure that the issues have not spread and that there is no threat to business. As an IT technician you have been tasked to investigate this and take appropriate actions.

SAMPLE

Task 1: investigate and take corrective action

Time limit

7 hours 30 minutes

You can use the time how you want, but all parts of the task must be completed within the time limit.

Brief

Tony has logged off the main system and has given you his laptop to work with. He has described the problems he has experienced when using his laptop as follows:

- applications are running slower than they used to
- programs are regularly freezing and not responding
- occasionally files are not opening

Firstly, you will be required to research what may be causing these issues.

You will then need to investigate and assess any vulnerabilities that may exist by analysing the emails and identifying any issue and possible resolution.

Finally, you will be required to identify actions that could be taken to resolve the issues.

(42 marks)

Instructions for students

Part A

In relation to this brief, firstly you must create a report to:

- discuss how these issues could be the result of either a cyber attack or an internal software program problem – you should clearly identify how you would differentiate between the two
- explain how and why the issues could have occurred
- identify the type of attack it could be

Part B

You have full administration rights and access to Tony's laptop (this will be a virtual machine assigned to you by your tutor).

Using the virtual machine (VM) you have been assigned, you must:

- log into the machine using the following credentials:
  - **username**: analyst
  - **password**: cyberops
- investigate the emails and assess any potential issues that may exist
- run a scan using the online tool **VirusTotal** to identify what attack, if any, has taken place

SAMPLE

In your report, you should:

- record your findings (this should include screenshots to evidence your investigation and use of the scan)
- suggest potential fixes for any issues that are identified

Part C

In your report, you should:

- provide an outline of any remedial actions that could be implemented to better protect the current system (for example, any additional security methods that could be used), including any future recommendations

Resources

For this task, you will have access to the following:

- word processor
- internet access
- virtual machine (provided by tutor)

Evidence required for submission to NCFE

Report document including evidence from parts A, B and C

SAMPLE

Task 2: ongoing maintenance

Time limit

2 hours 30 minutes

Brief

Following the resolution of the issues identified in task 1 you have been requested to produce a report that evaluates how ongoing maintenance will ensure the network and systems will remain secure and effectively operational.

Instructions for students

Create an evaluative report that:

- recommends ongoing maintenance measures that could be implemented to ensure the system remains secure and operational – this should ensure that the issues encountered in task 1 do not occur again in future
- recommends any remedial action you would take to ensure these measures are implemented and justifies the approach taken
- identifies the additional requirements to ensure these measures are manageable
- explores any systems upgrades that might be required based on these measures

(18 marks)

Evidence required for submission to NCFE

Written evaluative report.

SAMPLE

Document information

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2023.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of the Institute for Apprenticeships and Technical Education.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Post approval, updated for publication		01 June 2023
v1.1	Sample added as a watermark	November 2023	21 November 2023

SAMPLE